Senior Cyber Security Analyst
Information, Systems and Change

Overview	
Role Purpose	The Senior Cyber Security Operations Analyst is a pivotal role for the delivery of cyber security and all related tasks, both project and operational delivery to identify, protect and detect cyber threats and vulnerabilities across the entire Digital, IT and Data System Estate.
Responsible for	Supporting both the Heads of IT Systems and Cyber Security and Cyber Security Manager with the delivery of all security operational workload and projects as well as working with trends and analytics to look for unusual behaviours which could be a malicious software or the start of a cyber-attack using the security tools. Provide advice and support to the business on any IT security related matter in accordance with the Cyber Security Strategy
Reports to	Information Security Manager
Line management	N/A
Tier	
Expectation Level	Colleague
Role relationships	
Internal	Information Security Manager, Data Compliance Manager, Data Protection Officer, Information Asset Owners, Heads of Services, All Directors, Staff
External	Internal/External Auditors, Third-Party IT Service Delivery Suppliers

Role accountabilities

Your main responsibilities will be to assist the Cyber Security Manager in:

- Working with our vendors and internal teams to ensure the availability and correct functioning of IT security policies, procedures, and technology
- Working with the in-house applications team as well as third party providers to ensure continuous improvement and progress against agreed security practices.
- Assist in defining Security KPIs, and provide weekly and monthly reporting related to security KPIs, compile, and analyse data for management reporting and metrics
- Analyse and create remediation tracking activities against exploitable vulnerabilities discovered in the environment
- Identifying weak configuration areas for internet facing systems and cloud infrastructure and applications, performing vulnerability management, and scanning and coordinating and remediating penetration testing (automated and manual)
- Building response playbooks against cybersecurity trends and document security policies and processes for IT and Digital teams
- Lead and develop expertise in securing Azure cloud resources/workloads
- Review, monitor and improve network security on-prem and in Azure

Role accountabilities

- Review, monitor and improve security policies and processes within Microsoft 365, Exchange Online, Sharepoint Online and the M365 suite
- Monitor, maintain and respond to incidents and alerts within 365 Defender, Defender for Endpoint and Defender for Cloud
- Review and maintain Security baselines and configuration profiles for devices within InTune
- Review, monitor and advise on processes for patch management of endpoints, servers, applications, infrastructure, and hardware
- Design, document and implement role-based access, permissions and access control policies for securing hardware, systems, roles and identities, cloud resources, Active Directory/AAD, remote access and mobile devices, including PIM and elevated access
- Assist the Head of IT Security, IT Architects and Cloud Infrastructure teams in design, management, and implementation of cybersecurity projects
- Support and direct service delivery teams and business functions in implementing policy and processes to secure identities, hardware, software/systems and data
- lead in investigations and incident response and respond to cyber security incidents according to the cyber-security incident response policy, provide investigation findings to relevant business units to help improve information security posture, and validate and maintain incident response plans
- Provides guidance and oversight to other analysts, and work closely with SOC in handling security incidents
- Coordinate effort among multiple business units during response efforts and input to the BIA/BCP/DR Strategies and processes of business
- design and implementation of countermeasures or mitigating controls
- Research and assist in architecture of security solutions
- Close working relationship with governance and compliance teams
- Provide cyber security training and awareness for IT teams and business users
- Monitor cyber security related websites to stay up to date on current attacks and trends, and analyse potential impact of new threats and industry threat intelligence and communicate risks to relevant business units
- Work closely with other Housing Associations and cybersecurity teams in sharing knowledge, processes, and collective intelligence to improve own security posture
- Coordinating third-party cyber and information security assessments, improving processes and supplier management
  Mentoring Cyber Security Analyst and Apprentices in the Cyber Security Team.

The tasks and responsibilities outlined above are not exhaustive; the post holder may undertake other duties as is reasonably required.

To do the job well, we have outlined the knowledge, experience, and skills you need to do the job.

Personal Specification

Professional expertise (know how & experience)

Essential	Desirable
• Proven experience of working in a large and complex customer facing organisation and enterprise working environment, working with senior management, and presenting to groups of internal and external users/stakeholders	

• Experience of undertaking investigations, their resolution and capturing and embedding learning • Production and analysis of performance metrics • Working knowledge of data protection legislation including GDPR, principles of information security and governance (including NIST 800 and PCI-DSS)	

Skills	
Essential	**Desirable**
• Developing and managing relationships across IT and within the business • Strong influencing and negotiation skills • Good communication and decision-explanation skills and ability to build relationships • Documentation and report writing skills, and meticulous attention to detail • Ability to explain IT security risks to business stakeholders and be able to relate these to corporate risks • Understanding of threat and vulnerabilities modelling across the IT perimeter. • Presentation skills to higher management levels within the organisation • Manage simultaneously and conflicting priorities • Expertise in Microsoft Sentinel and KQL/threat-hunting • Expertise in Microsoft Windows Defender for Cloud, Mobile (Android and iPhone), and Endpoint (Server and Workstations), configuration, deployment, architecture, management, and reporting. • Expertise in Microsoft InTune and SCCM technologies for deploying security baselines, Antivirus technologies and configuration and compliance profiles • Expertise in networking security including firewalls, WAFs, NSGs, switches, WAPs, and routing protocols • Experience with SIEM/SOAR/MDR platforms and working with managed SOCs • Experience with SIEM implementation projects • Experience with vulnerability management and penetration testing tools (Tenable.io, Nessus Pro, Cymulate, Netsparker, SonarQube, MS TVM, Qualys) • Strong knowledge of operating under a zero-trust security methodology	

• Technical experience with Microsoft Identity and Access management (Azure Active Directory, Azure Active Directory premium solutions, Conditional Access, SSO, MFA, PIM). • Strong Knowledge of Microsoft Cloud App Security and related security tools • Technical understanding of the MITRE ATT&CK Framework and Threat Modelling • Desire to progress across the broader aspects of Information Security	

Qualifications and/or professional membership

Essential	Desirable
• In-depth knowledge of Red Team concepts such as reconnaissance, malware delivery and functionality, attack methodologies • In-depth knowledge of Information Security concepts and standards • In-depth knowledge and experience of Microsoft Azure infrastructure, architecture and security concepts and tools • Experience of ITIL Framework	• CEH qualification • CISSP qualification • Experience with Microsoft Cybersecurity Architect, Azure Security Engineer, Microsoft Enterprise/Security Administrator

NHG Expectations

NHG expectations framework outlines what we expect from our staff at the five different expectation levels we have across the organisation.

This role is a **COLLEAGUE** expectation level and therefore you should refer to the **COLLEAGUE** expectation profile in addition to this role profile.

The full NHG expectations framework is available on our external job site page and intranet, Milo.

You'll be assessed on the knowledge, experience, skills, and expectations criteria at various stages throughout the selection process.

Safeguarding

Any appointment to this post is conditional upon and subject to: ***(delete as appropriate)***	• Basic certificate (criminal record check) issued by the Disclosure and Barring Service (DBS)